

Computer Crime Investigators

A New Training Field

By BILL D. COLVIN
Special Agent
Economic and
Financial Crimes
Training Unit
FBI Academy
Quantico, Va.

Computer crime has been called by various names: Computer abuse, computer fraud, computer-related crime, and automatic data processing (ADP) crime. Regardless of the terms used to describe computer crime, it is where the "big money" is today in white-collar crime, with corporate computer crime losses averaging \$621,000¹ per incident.

Law enforcement officers can be trained to investigate competently, professionally, and successfully 93 percent of all computer crimes, and to recognize the level of technical expertise required in a consultant to solve the remaining 7 percent, as will be demonstrated.

The Economic and Financial Crimes Training Unit of the FBI Training Division has conducted extensive research into the training needs of

computer crime investigators. The research is based on an analysis of computer systems to determine the areas of vulnerability and the methods of penetration.

A typical computer system uses programs (instructions) to enter data (alphabetic or numeric material) via an input device to a central processing unit (CPU), where the data is processed and output produced, which ultimately becomes information. It is this flow, input/processing-output, that is basic to all computer systems. To facilitate this flow, there must be some form of auxiliary storage (magnetic disk and/or tape), a console unit (which allows communication between the CPU and the computer operator), and terminals (which allow remote access to the computer system). The unshaded portion of figure 1 illustrates this computer system.

Areas of Vulnerability

The shaded portions of figure 1 represent the areas of vulnerability in a

(Published by the Federal Bureau of Investigation, U.S. Department of Justice)
Reprinted from the FBI Law Enforcement Bulletin, July, 1979

computer system. As is evident, input can be altered; computer programs can be altered or created; CPU's can be misused; data contained in auxiliary storage files can be added to, changed, or deleted from; output can be altered; operating systems can be modified to allow perpetrators control of the computer; and computer communications can be intercepted or altered.

Computer Crime Schemes

The areas of vulnerability identified in figure 1 can be considered as computer crime schemes and can then be ranked according to the technical difficulty required to commit the crime. In ascending difficulty, the ranking is:

1. Input/output alteration,
2. Computer operations,
3. Computer programs,
4. Auxiliary storage manipulation,
5. Operating system penetration, and
6. Computer communications.

The alteration of input/output would be the least technically difficult scheme used to commit a crime, while the interception or alteration of computer communications is the most technically difficult crime scheme. By

analyzing these schemes in terms of technical capabilities, computer crime suspects can be developed.

Computer Crime Suspects

Within any data processing organization there are only four basic functions performed: (1) Data entry, (2) machine operations, (3) application programming, and (4) systems analysis. Computer personnel are assigned to work in one of these four basic functions depending on education

“Law enforcement officers can be trained to investigate competently, professionally, and successfully 93 percent of all computer crimes . . .”

level, experience level, needs of the organization, and other miscellaneous factors. The data entry function is the least skilled area with the greatest number of persons assigned and the systems analysis is the most skilled area with the least number of persons assigned. It is these identifiable skill

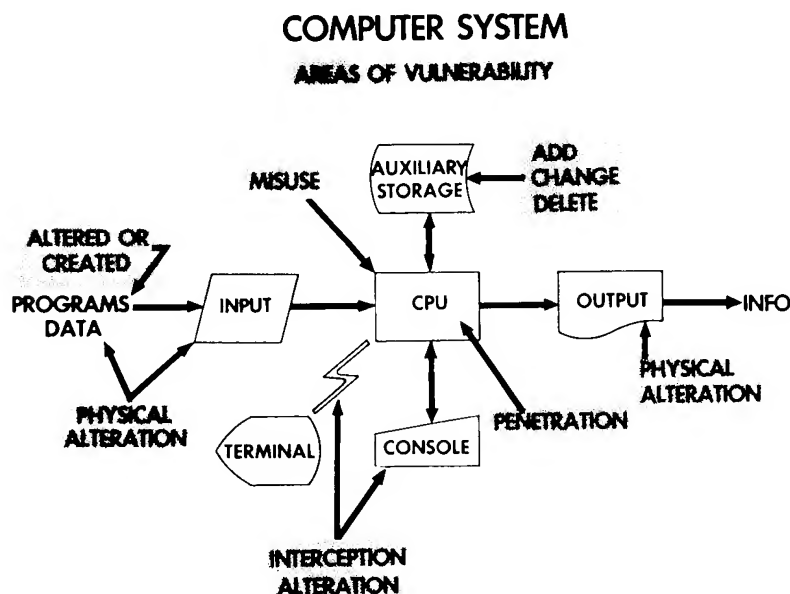
levels, or personnel capabilities, that allow computer crime suspects to be developed. As illustrated in figure 2, personnel having systems analyst capabilities are capable of perpetrating crimes in the most sophisticated scheme levels, computer communications, and operating system penetration.

The process of being able to identify the crime as occurring in either crime scheme 5 (operating system penetration) or crime scheme 6 (computer communications) assists the investigator in developing suspects and narrowing the scope of the investigation. At these levels, only the more skilled personnel will have the technical ability to commit crimes. The more skilled the job function, the fewer the number of personnel capable of performing that job. If the crime scheme is identified as a computer program, then figure 2 shows that the suspects are programmers and systems analysts. Personnel in both functions possess this technical capability. Investigators identifying crime schemes in the input/output alteration level have a broad range of suspects. Figure 2 points out that not only data entry personnel are technically capable of criminal activity at this level, but also everyone else in the organization with that technical capability. It is important then for the investigator to be able to recognize the highest technical level at which the scheme was perpetrated in order to narrow the scope of the investigation. Investigators must be trained not only in how to investigate computer crimes, but also in how to recognize the type of scheme used.

Training Levels

The training needs of the computer crime investigator can be stated in terms of three training levels: (1) An awareness level, (2) a comprehensive level, and (3) a specialist level. Figure 3 illustrates that these training levels can be applied to the schemes of computer crime to determine the level of training needed by the investigator to

Figure 1. Today's computer systems are totally vulnerable.



FEDERAL BUREAU OF INVESTIGATION
INVESTIGATIVE TECHNIQUES
OF
COMPUTER-RELATED CRIMES

I. General Information

This course is four weeks in length and is conducted at the FBI Academy in Quantico, Virginia 22135, (703) 640-6131.

The entire curriculum is centered around the investigations of automated financial record systems. A live banking application consisting of Demand Deposits, Installment Loans, Savings, and Certificates of Deposits is used as the data base. To give the student a realistic approach, frauds have been purposely built into the system, each requiring various degrees of sophistication to investigate. Although the course is banking oriented, the concepts learned can be applied to other computer-related crimes, as well as the use of the computer in case investigations. Much "hands-on" experience is emphasized.

II. Course Objectives

1. To provide the investigator with sufficient competence in the methods and techniques of investigating in an EDP environment to conduct the investigation professionally.
2. To provide the investigator with an in-depth and specific understanding of computer facilities, organization, documentation, controls, security measures, and computer audit techniques.
3. To provide the investigator with techniques which can be used for the successful investigation of computer-related crimes.

III. Course Schedule

1st Week

Introduction to Data Processing; Coding Schemes; Computer Operations; Card Utility Programming; Computer Operation Control Language; Data Organization; Introduction to RPG II; Programming; Computer Programming Problems; Computer Fraud Practical Problems; Computer Workshops.

2nd Week

Computer System Documentation; Magnetic Disk Storage and Concepts; Data File Security; Disk Utilities; Computer Programming Problems; Computer Fraud Practical Problems; Computer Workshops.

3rd Week

Magnetic Disk Programming; Multiple I/O Programming; Computer System Documentation; Micro Computers; Teleprocessing; Data Communications; Computer Systems Vulnerability; Computer Programming Problems; Computer Fraud Practical Problems; Computer Workshops.

4th Week

Computer System Documentation; Computer Programming;
Computer Core Dump; Search Warrant Practical Exercise; Evidence in
Computer-Related Crimes; Advanced Computer Concepts; Computer Programming
Problems; Computer Fraud Practical Problems; Computer Workshops.

conduct a professional investigation. In addition, training programs must consider these evidence problems: Sources, recognition, obtaining, and preservation.

The first level of training for a computer crime investigator is the awareness level, which addresses the least sophisticated computer crime schemes. As indicated in figure 3, this training program will provide the investigator with the technical knowledge to investigate successfully computer crimes involving input/output alteration and computer operations. The source of evidence in cases involving input/output alteration is the source document. In cases where computer operations are involved, the source of evidence is frequently the console log. Since training must involve teaching the investigator how to obtain evidence, this level training must stress terminology, recognition and understanding of source documents, and the availability of information from console logs.

The second level of training, the comprehensive level, must concentrate on computer crime schemes involving computer programs and the

manipulation of auxiliary storage. As indicated in figure 3, the source of evidence in computer crime schemes involving computer programs may in fact be a source program and a corresponding object program. The sources of evidence for computer crime schemes involving auxiliary storage manipulation are found in job accounting systems and system documentation. Therefore, this comprehensive level training program must provide the investigator with the technical skills to

“ . . . and to recognize the level of technical expertise required in a consultant to solve the remaining 7 percent . . . ”

understand the complexities of computer programs, how to locate the programs, how to distinguish between a source program and an object program, and the importance and function of each.

The investigator must be able to obtain various types of documentation

and be prepared to use the documentation as an investigative aid, in addition to being able to decipher job accounting logs. By its very design and position in the hierarchy of training levels, the comprehensive level training program provides the investigator with the technical skills to investigate computer crime schemes ranging from input/output alteration to auxiliary storage manipulation. It must also exceed this level and address the operating system penetration and computer communications schemes.

The third level of training is the specialist level. It is the most sophisticated training level (and rightfully so) since it is designed to combat the computer crime schemes involving the penetration of operating systems and the alteration or interception of computer communications. The sources of evidence in these cases are often located in communication logs, communication system documentation, or other sophisticated areas.

Computer crimes perpetrated in this training level are so sophisticated, and the technology used so dynamic that it changes almost daily, that only practicing, competent computer spe-

Figure 2. The computer crime scheme can be used to identify suspects by technical capability.

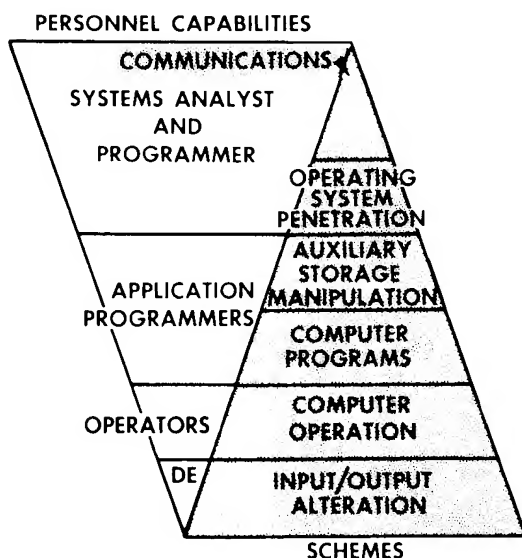
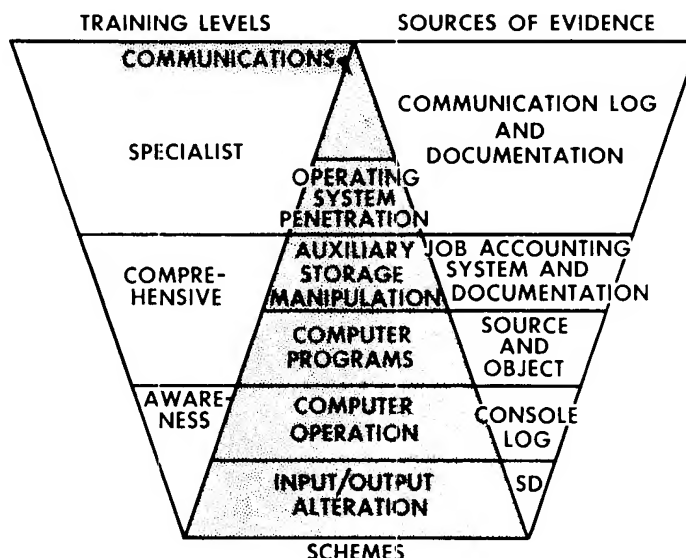


Figure 3. Identifying computer crime schemes can guide the investigator to sources of evidence, while training programs can focus on recognizing, obtaining, and preserving that evidence.



cialists feel at ease in this area. Rather than design a training program to provide the investigator with the highly sophisticated technical skills needed to investigate this level computer crime scheme, another approach is more practical. (Even if the investigator were trained at this level, the technical skills would be lost or outdated almost immediately due to the rapidly changing technology and the investigator's inability to devote full time to this field.) During the comprehensive level training program, the investigator can be made aware of the type of computer specialist needed to assist and consult in the various schemes being perpetrated at the specialist level, as well as the sources of evidence. In this manner, the investigator can maintain control over the case and direct the activities of the computer specialist.

To determine the number of personnel to commit to such training, knowledge of the distribution of cases and the length of such training programs is necessary.

Distribution of Cases

Research conducted at the FBI Academy indicates that the number of

occurrences of computer crime is greatly reduced by the degree of technical ability required to perpetrate the scheme. The majority of the cases occur in the input/output alteration level, while very few cases are known to have occurred in crime scheme 6 (computer communications). Figure 4 indicates that 58 percent of the detected computer crimes occur in schemes 1 and 2, input/output alteration and computer operation, respectively; 35 percent of the cases occur in crime schemes 3 and 4, computer programs and the manipulation of auxiliary storage; and 7 percent of the cases are in schemes 5 and 6, operating system penetration and computer communications. This distribution of cases manifests the types of training programs needed.

Of these schemes, computer programming appears to be the fastest growing scheme and is taking on a new look. In the early stages of research, it was found that legitimate computer programs were often later altered to commit a crime. More recently detected, entire computer programs are being prepared for no other purpose than to commit a crime.

Training Programs

Training can thus be set up in terms of three levels of sophistication. An awareness-type training program, as taught by the Federal Bureau of Investigation, lasts 5 days and gives the investigator the technical skills necessary to investigate 58 percent of the cases (as indicated in figure 4). Although this is the level of the majority of the crimes, monetary losses are frequently insignificant or negligible.

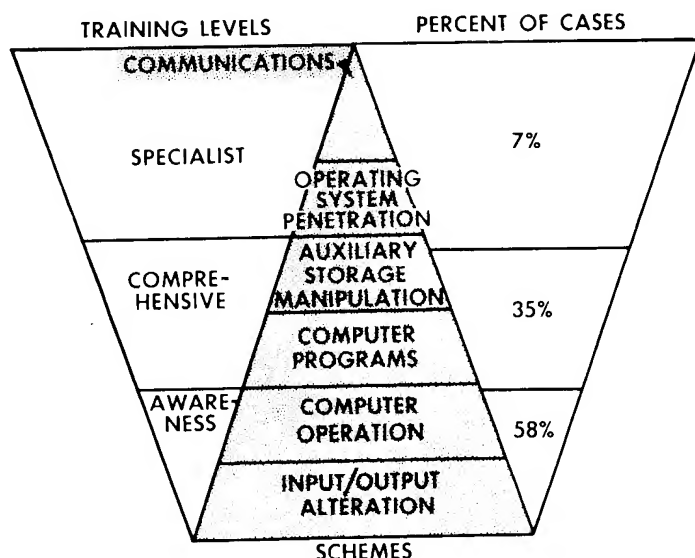
Quality cases or crimes involving large and significant monetary losses appear to be occurring in training level 2, which is a comprehensive training level. The FBI's comprehensive level training program lasts 4 weeks. The investigators who complete this training program are then given refresher training approximately every 18 months to maintain and update their technical skills.

Through training in the awareness and comprehensive levels, 93 percent of the computer crime cases can be successfully, competently, and professionally investigated (as indicated in figure 4).

Those few investigators receiving the comprehensive training are also taught to recognize the crime schemes being perpetrated at the specialist level. This training provides the investigator with the technical skills to maintain control over and direct the investigation, using the consulting services and assistance of a computer specialist.

Training programs for investigators of computer crimes must be carefully designed and administered to provide the investigator with the technical skills to investigate computer crimes professionally without making him or her a computer specialist. **FBI**

Figure 4. Investigators can be trained to investigate successfully 93 percent of all computer crimes, while maintaining professional control over the remaining 7 percent.



Footnotes

¹ Congressional Record Proceedings and Debates of the 96th Congress, 1st sess., Vol. 125, No. 7, January 25, 1979, p. S 726